TEXAS
Health and Human Services

Risky Business

An honest look at assessing risk

John Skaarup, CISSP

Deputy Chief Information Security Officer

Texas Health and Human Services

In Brief (Who is this for?)

1. Applicability
   a. State Agencies (TAC 202)
   b. Anyone doing business with Federal Confidential Data
2. Anyone handling Confidential or Personal data
3. Anyone
4. You

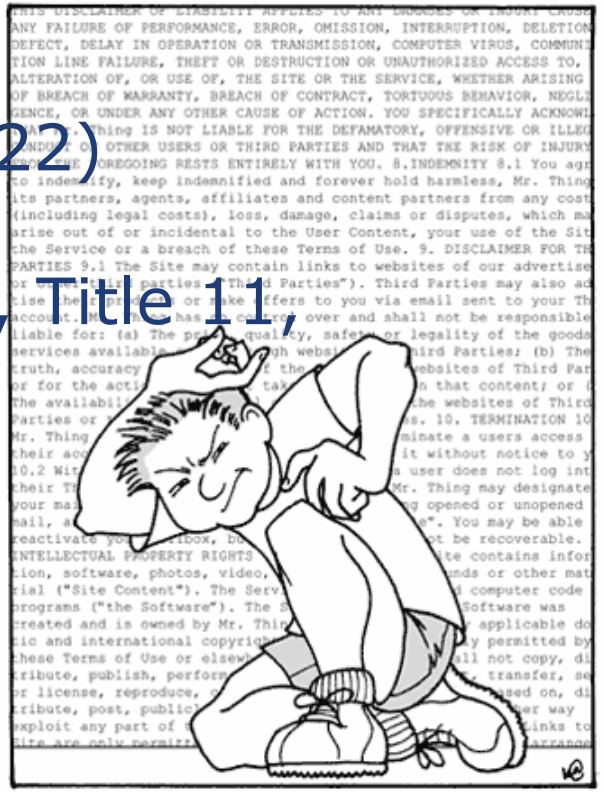
TEXAS
Health and Human Services

NIST RMF


RMF
Compliance
Life Cycle
01
Categorize
System
02
Select
Security
Controls
03
Implement
Security
Controls
04
Assess
Security
Controls
05
Authorize
System
06
Monitor
Security
Controls

State Regulations

- Texas Administrative Code, Title 1, Part 10, Chapter 202
- Texas Penal Code, Title 7, Chapter 33
- Texas Medical Records Act (SB11)
- Texas Public Information Act of 1999
- Texas Identity Theft Reporting (SB 122)
- Texas Cybersecurity Bill (HB 8)
- Texas Business and Commerce Code, Title 11, Sub. B, Ch. 521



Federeal Regulations

- Health Insurance Portability and Accountability Act
  - 45 CFR Parts 160, 162, and 164
  - Omnibus Rule
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
- IRS/FTI Publication 1075
- Centers for Medicare & Medicaid Services (CMS) – Affordable Care Act (ACA)
  - Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E Suite)
  - Information Security and Privacy - Acceptable Risk Safeguards (ARS)
- Federal Information Security Management Act (FISMA)
- Social Security Administration (SSA)
- Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration
- Criminal Justice Information Services (CJIS) Security Policy
- Family Educational Rights and Privacy Act
- 34 CFR Part 99
- Computer Fraud & Abuse Act of 1986
- Patriot Act
- Computer Security Act of 1987
- Homeland Security Act


Business
I.T.
Risk
A. Barkley

Simplified

1. What do you have?
   - *FIPS 199; NIST SP 800-60; NIST SP 800-53r4 (PM-5 Information System Inventory)*
2. How are you supposed to secure it?
   - *FIPS 200; NIST SP 800-60; NIST SP 800-53r4; A lot of others*
3. Are you doing it?
   - *NIST SP 800-70; NIST SP 800-53r4; A lot of others*
4. What did you miss?
   - *NIST SP 800-53A*
5. Ready to use it?
   - *NIST SP 800-37; NIST SP 800-53r4 (CA-06 Security Authorization)*
6. Keep an eye on it?
   - *NIST SP 800-37; NIST SP 800-53r4*

TEXAS Health and Human Services

What do you have?

- Inventory & Categorization

What do you have?

- Inventory & Categorization

Our Conversations go like this…

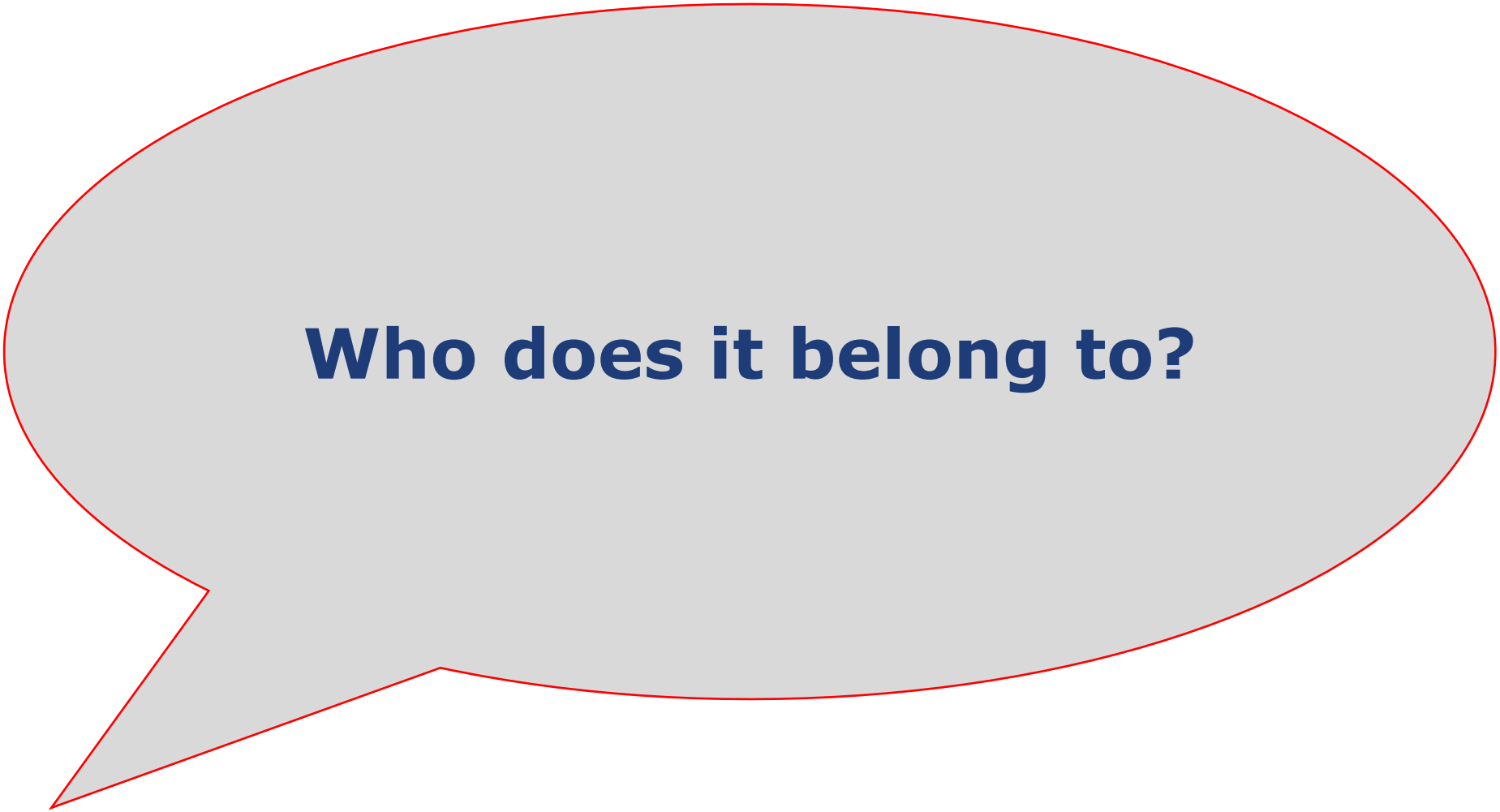
What do you have?

Hey, we should (turn-off / retire/ decommission) that old system!

What do you have?

Oh No, no, no!
(*We don't know what's on it or <u>what will break if</u> we do*)

What do you have?



What do you have?

Dunno. Let's turn it off and *see who screams*...

What do you have?

Simply put:

- **If you don't know what you have you can't measure risk**

  …and other problems will arise

What do you have?

Inventory & Categorization:

- Categorization is based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals
- Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization

What do you have?

Categorization for Texas Agency's:

- Low baseline
- Moderate baseline
- High baseline

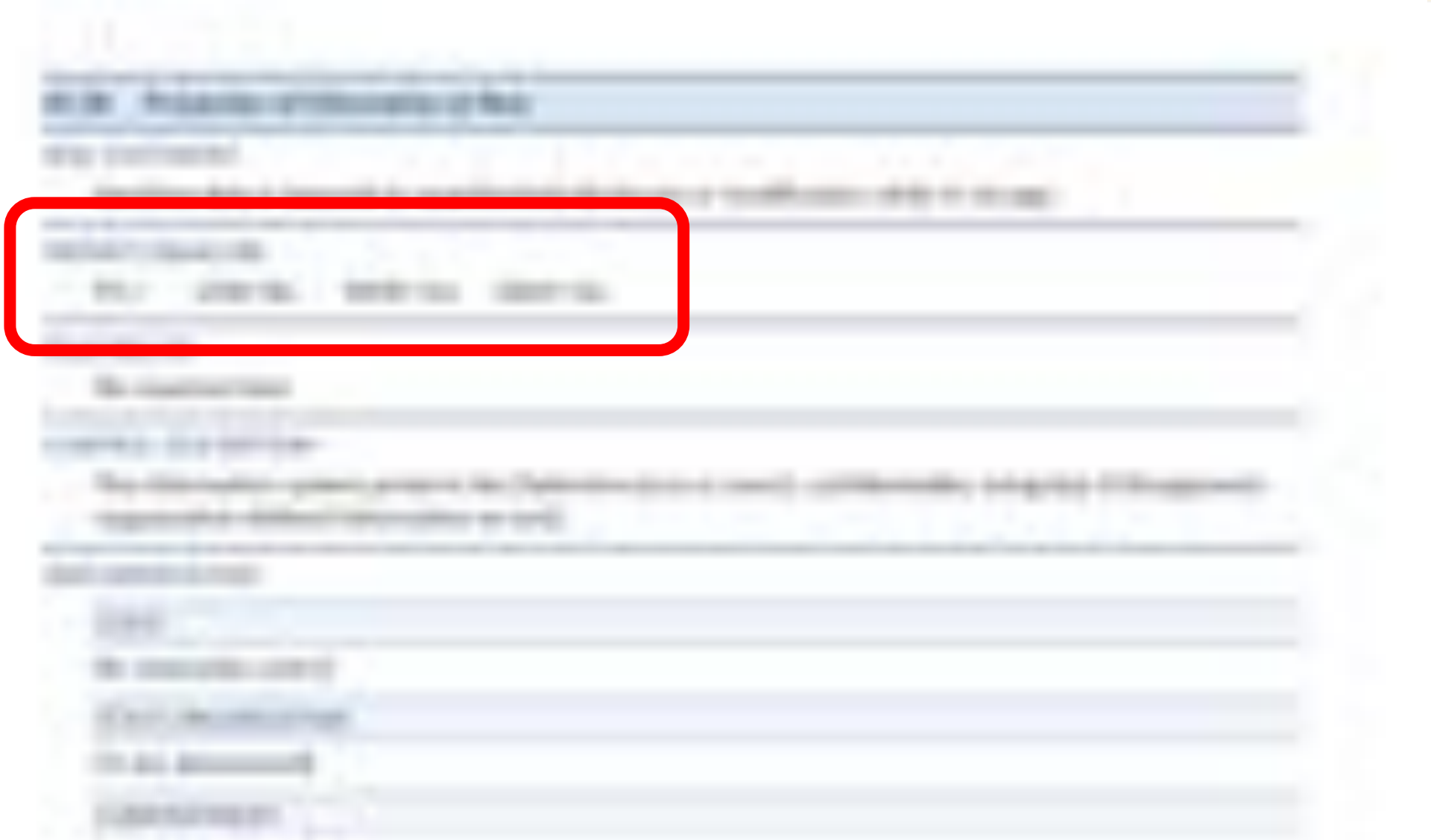
How are you supposed to Secure it?

- Selection of Security Controls

Understanding requirements

What do you have?

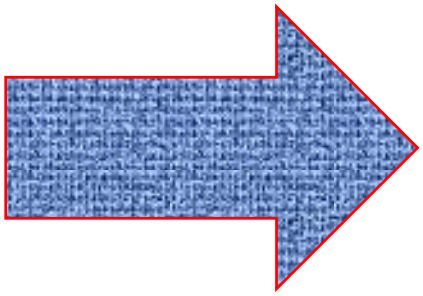
TEXAS
Health and Human Services




I DON'T THINK
YOU UNDERSTAND MOM
I NEED LIGHTUP SHOES
SO I CAN RUN FASTER

Are you doing it?

- Implementation of Security Controls



What did you miss?

- Assessment of Security Controls
  - Risk Assessment vs. Security Assessment

A self-assessment against documented controls conducted by the Information Owner

A validation of the completed Risk Assessment (by a trained/certified Security professional)

What did you miss?

findings...

POA&M

- Plan of Actions and Milestones

(AKA: a “corrective action plan”)

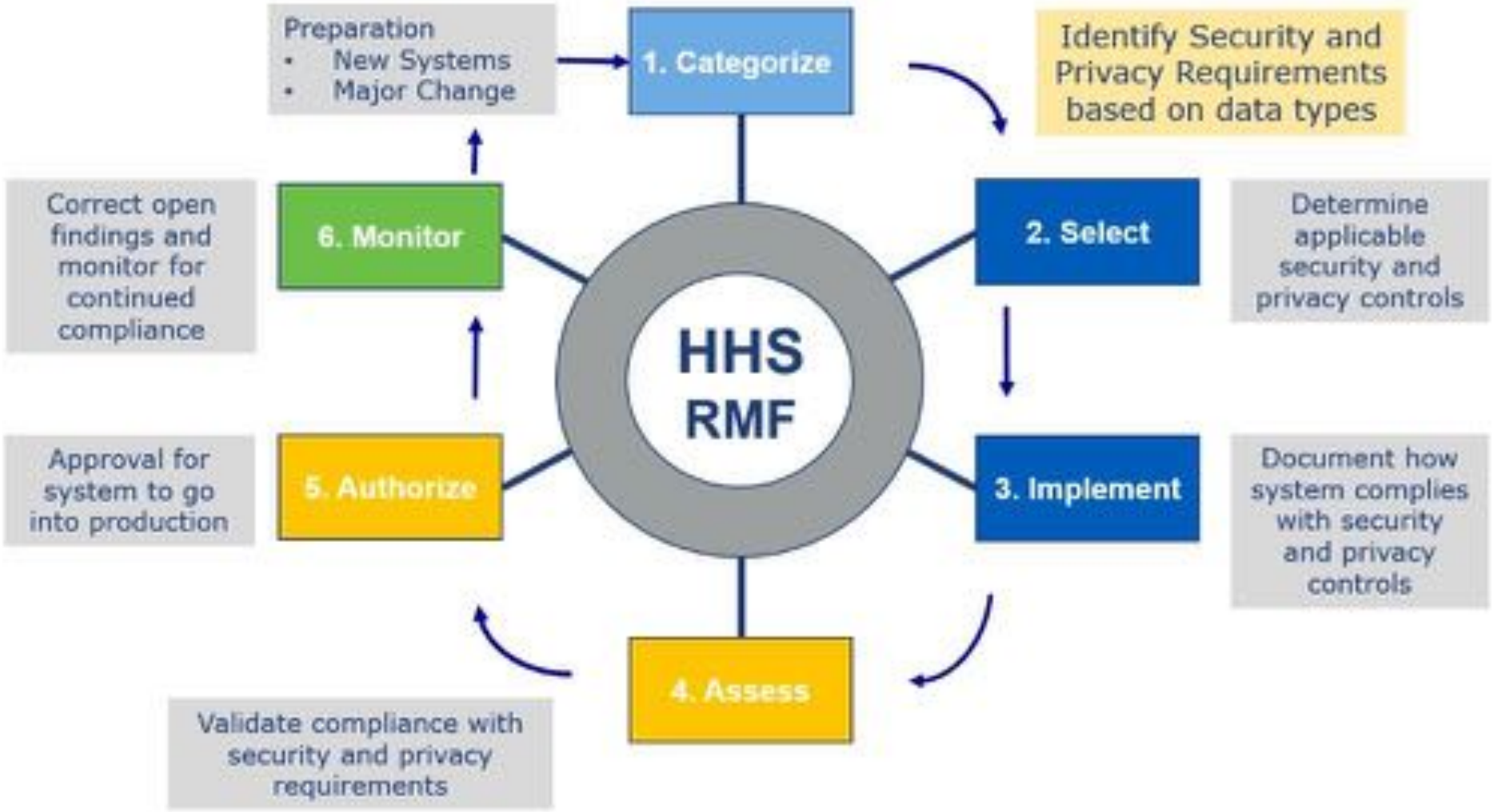
Ready to use it?

- Authorize Information System
  - Authority To Operate (ATO) process

Keep an eye on it?

- Establishment of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate.

Charts


Preparation
• New Systems
• Major Change
1. Categorize
Identify Security and Privacy Requirements based on data types
2. Select
Determine applicable security and privacy controls
3. Implement
Document how system complies with security and privacy controls
4. Assess
Validate compliance with security and privacy requirements
5. Authorize
Approval for system to go into production
6. Monitor
Correct open findings and monitor for continued compliance
HHS RMF

Obligatory Q&A Slide

TEXAS
Health and Human Services

Thank you

Your contact information here